International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 17
July 2018

Enhancing user experience by extended Fraud Detection ranking approach

K. Naveena
[1]M.Tech, Department of CSE, JNTUACE, Anatapur, A.P.

Email: [1]<naveenaroyal99@gmail.com>

Abstract-

Dishonest activities in App Store, the most favoured app market, propellant search rank mishandle and lead to malware growth. To recognize malware, earlier effort has made awareness on app executable and agreement scrutiny. Here, we initiate SSPA, a novel system that determines and controls suggestions left behind by fraudsters, to detect both malware and apps focused to their content fraud. SSPA demonstrated the reliability and individually combines perceived apps with linguistic and behavioural signals gathered from app store to identify apprehensive apps. SSPA accomplishes over 95% accuracy in classifying gold standard datasets of malware, deceptive and legal apps. SSPA realizes hundreds of deceptive apps that currently avoid App Store detection technology. SSPA also helps to determine the malware add-on to the existing and popular apps that implemented a specific kind of verification approach.

Keywords:

Android market, search rank fraud, malware detection,Online social games, Sociability, In-game aggression, Abusive behavior, Chat analysis, Machine learning

1. INTRODUCTION

The development of Android app markets such as Google Play [1] and is the stimulus model to admired apps, make them enticing targets for subtle and malignant

activities. Some subtle developers deceitfully update the search rank and influence of their apps [2], while malignant developers use app markets as a inaugurate packing [12] for their malware [3] [6]. In Google Play Store, it affords services that user can determine the precise application [4] [5], buy those applications and install them on their mobile devices. As Android is open source environment all the specifics about the application. Based on that users can easily find by the application developers through Google play. These leads to good chance of implementing malware to the applications that impact mobile devices used by the users. Google play store employs security system known as Bouncer system [6] to delete the vicious apps from its store. Therefore, this technique is not effective, as testing some apps using virus tools for many apps are found as malicious which are not disclosed by Bouncer system [6]. Subtle developers use search ranking algorithm to strengthen their apps to the top against the fact that searching. Emerging to download mobile apps from Google play store, users are asked to give the ratings and reviews about those downloaded applications. Yet subtle developers give false ratings and review about their application to promote it to the top position. There are two unique approaches used for identifying malware in Google Play. Those approaches are Static and Dynamic. The active approach requests apps to be in a safe situation. The mobile industry is developing rapidly; therefore the mobile usage is increasing in the market. Different App stores like Google play store and Apple store launched their leader board on daily basis to encourage the users to download most popular applications by observing the ranking of applications. In fact, it is an effective to advertise particular mobile applications. An app which has large number of downloads will obtain huge profit [2]. In order to have their Apps ranked as high as possible, app developers promote their apps using various ways such as advertising, offers etc. Such applications dent to phone and also may cause data pilfering. So we are proposing an android application which will process the

information, comments and three reviews of the application with natural language processing to give results. So it will be easier to decide fraud application.

2. RELATED WORK:

2.1. Android Bouncer:

Android Bouncer [7] is a best scanning mechanism technique which is helpful to perform operations automatically majorly for malicious software without creating any problem to the user. The service carried out various set of analyses on specific kind of applications which are already located in Android Market as well as. Whenever the application is installed, the service immediately begins analyzing procedure to know any kind of attacks are there.. The problem with this technique is we may not get precision data from the webservers.

2.2. Survey on Web Spam Detection: Principles and Algorithms:

Search engines [8] are the main sources to acquire any information on the web. previous research techniques includes a special kind of information retrieval techniques and also it benefitted for areas like academics and industry. This technique represents a specific kind of review majorly for spam detection on web based on some algorithms. We divide all the prior algorithms into three types based on the type of information it holds: content-based methods, link-based methods, and methods based on non-traditional data such as the behavior of a user. We can also again sub divide link-based category into five types based on ideas and principles which we have used. We can also determine the concept of web spam numerically and carry out a brief survey on various spam forms. The problem with this technique is these describes only positive and negative reviews , for detection of malware.

2.3. Fair Play:

FairPlay, is a leveraging kind of technology[9] [10] which is helpful in detecting fraud kind of issues in Google Play. To detect fraud activities, we need to generate some kind of relational, behavioral as well as linguistic features. We can also able to find some apps which includes unbalanced review, and rating. These tools works for only positive and negative reviews helpful for detecting malware. The problem with this technique is Data will be personalized by hackers or unauthorized persons in web pages.

3. PROPOSED WORK

Introduction of Fraud detection techniques for mobile application act as a best solution for above problem. We collect social identification number of app vendors for security purpose to identify if they upload any malware. Resource constraints can contain attackers to submit malware within a short period of time. Loyal users may be affected by malware which leads to uncomfortable experiences in their reviews. Then there is a chance of making app as suspicious/malware. Mainly its responsibility is to prevent the display of Web contents from hands of attackers. who are

It determines fraud detection framework system that works effectively in detecting the fraud or malware activities performing on Google Play. We detect this activities based on the application evidence such as rating, ranking and review evidence will be checked by an unsupervised evidence-aggregation method to evaluate the credibility of mobile Apps. comparing to other prior techniques this mechanism works fine better for the end user.. There is a chance of User to review after they download that specific application using their account from app store.

3.1. METHODOLOGY

To perform safe operations of Web-based systems in Web environments. This is done mainly to save the reputation of organizations from cyber-attacks and to make sure

whatever the operations we are performing in web are safe based on the integrity monitoring. We represent this in the form of applicability and practicality of the proposed system. We can also determine time metrics, specifically which are in relation to its computational overhead presented at the Web server, as well as the overall latency from the clients' point of view, based on various Internet access methods.

Web Server

In this particular module, the Web Server needs to login by providing valid user name as well as password. Whenver login operation is successful he is able to do some sort of operations such as Authorize, Add Filter, View all Mobile Manuals, View all uploaded apps with rank and ratings details, View all Apps with review, co review and Recommend details, View all Search Rank Fraud User, View all Malware details for Apps,.

Apps Developer

Add App

In this module, the admin has a capability to add the applications. If the admin thought to add new app, he has to enter application name along with app description, type of mobile, users, file name, images related to application and finally has to click on register button. Then the information will be store in a database.

View application

In this module, when the admin clicks on view application, it should display the application name along with app description, type of mobile, users, file name, application images related to application.

Evidence for frauds

In this module, when admin clicks on evidence for fraud details, user name, type of mobile, application name, application ID, fraud IP address, fraud system name, date and time will be displayed.

User

In this module, n number of users can access and perform operations. User has to register first to perform any kind of operation. After the completion of registration procedure he has to login by providing valid kind of user name and password. After login procedure he can be able to do perform some sort of operations like ,Viewing Profile, Adding Mobile name/Select mobile name and Upload apps with Appname, App logo image, Add mobile booklet like Select mobile name and OS and attach Mobile Manuals file, View all uploaded apps with rank and ratings and Mobile Manuals

Search and download mobile apps

In this module user can able to search the type of mobile and when we click on search then he can able to see a page which contains application name, application images, view details of mobile app, enters application ID enter the secret key and download the file. and send response to user.

Search for top K applications

In this module, user enter the application name and has to choose the top N details then we get the details about leading app like name of application, description of application, type of mobile, users, file name, images related to that specific application along ratings of that particular application also will be displayed.

4. PERFORMANCE EVALUATION

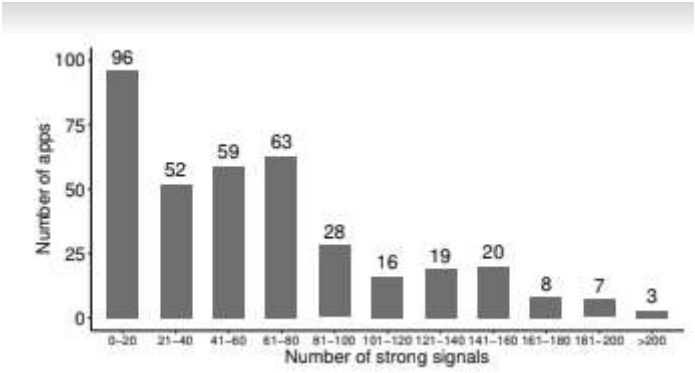

Fig 1. Distribution of the number of malware and fraud indicator words in the reviews of the 372 identified fraudulent apps (out of 1, 600 apps). Around 75% of these apps have at least 20 fraud indicator words in

their reviews.

The above figure explains the number of malware and fraud activities detected in fraudulent apps. These can be identified based on the reviews. Nearly in 372 fraudulent applications [11], malware and fraud activities have detected. Around 75% of the apps contains 20 fraud indicator words in their reviews.

5. CONCLUSION

we implemented a fraud detection system for mobile Apps as a part of proposed approach. We use to detect the fraud activities based on ranking and rating. Mainly, we proposed an optimization technique to check all the kind of evidences to evaluate the credibility of mobile Applications. Therefore, it is an easy way to extend this with some other evidence to identify fraud ranking. Finally, we verify the proposed system based on some results of real-world App data which are gathered from the App Stores. We carry out more effective fraud identifying system in future and it will be more helpful in analyzing the rating, review, and rankings. We will enhance our ranking fraud detection approach based on mobile Apps recommendation, for obtaining better user experience.

REFERENCE

[1]Alaa Salman Imad H. Elhajj Ali Chehab Ayman Kayss, IEEE Mobile Malware Exposed.International Conference on Knowledge discovery and data mining, KDD'14 pages 978- 983.

[2]Alfonso Munoz, Ignacio Mart ˜ ´ın, Antonio Guzman, Jos ´ e Alberto Hern ´ andez, IEEE Android malware detection from Google Play meta-data: Selection of important features.2015, pages,245-251.

[3]Chia-Mei Chen, Je-Ming Lin, Gu-Hsin Lai,IEEE Detecting Mobile Application Malicious Behaviors Based on Data Flow of Source Code.2014 International Conference on Trustworthy Systems and their Applications pp 95-109.

[4]D. F. Gleich and L.-h. Lim. Rank aggregation via nuclear norm minimization. In Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining, KDD '11, pages 60–68, 2011.Y.T. Yu, M.F. Lau, "A comparison of MC/DC, MUMCUT and several other coverage criteria for logical decisions", Journal of Systems and Software, 2005, in press.

[5]E.-P. Lim, V.-A. Nguyen, N. Jindal, B. Liu, and H. W. Lauw.Detecting product review spammers using rating behaviors. In Proceedings of the 19th ACM international conference on Information and knowledge management, CIKM '10, pages 939–948, 2010.

[6]N. Jindal and B. Liu, "Opinion spam and analysis," in Proc. Int. Conf. Web Search Data Mining, 2008, pp. 219–230.

[7]J. Oberheide and C. Miller, "Dissecting the Android Bouncer," presented at the SummerCon2012, New York, NY, USA, 2012.

[8]K.Shi and K.Ali. Getjar mobile application r ecommendations with very sparse datasets. In Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining, KDD '12, pages 204–212, 2012.

[9]J.Kivinen and M. K. Warmuth, "Additive versus exponentiated gradient updates for linear prediction," in Proc. 27th Annu. ACM Symp. Theory Comput., 1995, pp. 209–218.

[10]N. Spirin and J. Han. Survey on web spam detection: principles and algorithms. SIGKDD Explor. Newsl.,13 (2):50–64,May2012

[11]IanFellows, http://cran.r-project.org/ web /packages /wordcloud/ wordcloud.pdf.

[12] Feinerer, I., & Hornik, K. (2012). tm: Text Mining Package. R package version 0.5-7.1.